ABSTRACT OF THE DISCLOSURE

A block encryption method and schemes (modes of operation) that provide both data confidentiality and integrity with a single cryptographic primitive and a single processing pass over the input plaintext string by using a non-cryptographic Manipulation Detection Code function for secure data communication over insecure channels and for secure data storage on insecure media. The present invention allows, in a further aspect, software and hardware implementations, and use in high-performance and low-power applications, and low-power, low-cost hardware devices. The block encryption method and schemes of this invention allow, in yet a further aspect, encryption and decryption in parallel or pipelined manners in addition to sequential operation. In a yet further aspect, the block encryption method and schemes of this invention are suitable for real-time applications.